UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/689,000	10/21/2003	**Yair Shachar**	NAPEVC-6221-US	4369

28481 7590 08/27/2008

TIAJOLOFF & KELLY
CHRYSLER BUILDING, 37TH FLOOR
405 LEXINGTON AVENUE
NEW YORK, NY 10174

EXAMINER	
MOORTHY, ARAVIND K	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
08/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/689,000	SHACHAR ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 May 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60* is/are pending in the application.

4a) Of the above claim(s) *43-60* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *see attachment*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the communications filed on 12 May 2008.

2. Claims 1-60 are pending in the application.

3. Claims 1-42 have been elected in response to a restriction.

4. Claims 1-42 have been rejected.

5. Claims 43-60 are non-elected claims.

Information Disclosure Statement

6. The examiner has considered the information disclosure statement (IDS) filed on 21 October 2003.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-10, 14-16, 19-21, 23-27 and 30-39 are rejected under 35 U.S.C. 102(e) as being anticipated by Monroe US 2003/0025599 A1.

As to claim 1, Monroe discloses a method comprising:

collecting security data (i.e. forwarding the event to selected stations on a network. Basically, the location, type and priority of event are "tagged" at the point where a sensor picks up the event and event data is then forwarded only to selected stations on the network as required by a priority hierarchy. This permits a

large amount of data to be collected at the site of a sensor while minimizing transmission of the data to an "as-needed" basis, reducing the overall bandwidth requirements of the system. As an example, while periodic data may be gathered at a sensor, only data indicating a change in condition will be transmitted to various monitoring stations. In addition, monitoring stations are selected based on pre-established hierarchy, typically managed by a system server) [0108];

providing the security data to a first security station [0108];

selecting at least a second security station [0159];

providing the security data to the at least second security station so that the first security station and the at least second security station have concurrent access to the security data (i.e. One of the important features of the system is that legacy devices may be incorporated into the system whereby the signals generated by such devices may be transmitted, archived, and retrieved using the management methods of the subject invention. This is particularly useful when the system is installed as a retrofit to update existing systems having various legacy devices such as, e.g., fire alarms, motion detectors, smoke sensors, fire sensors, panic buttons, pull alarms and the like. The system is also useful when used in combination with legacy closed-circuit analog security cameras. In the case of the cameras, the signal is digitized prior to transmission. With specific reference to FIG. 6, the system is adapted to incorporate one or more legacy devices 100, which are basic ON/OFF devices adapted for generating a signal when a monitored event occurs. This can include, but is not limited to, motion sensors,

door contacts, smoke and fire detectors, panic buttons or pull alarms, and the like. As is typical of these devices, they often provide a local signal such as a siren or other sound signal at the site of the device and in some cases send an activation signal to a remote, hard-wired location. In the present invention, these devices are connected to the network and the activation signal is sent over the network when the device is activated. Using the above described management techniques, the signals are identified for location, time, and type of signal. This is then sent to the central server 8 and monitor server 6 (see FIG. 1) for management of the event and the related activation signal. Basically, and as will be further explained herein, the activation signal(s) are transmitted via a network to the server systems, which include the event logging function 102, appropriate filters 104 and a notification processor 106 for prioritizing the event and managing the transmission of an event signal to selected monitoring and archiving stations on the network. Specifically, it is important to note that once the signal identification, transmission and management methods of the subject invention are incorporated, the system is readily and equally adapted to manage the various network security appliances designed for the system, digital camera systems, and the legacy analog cameras and security devices of the prior art.) [0159]; and

opening a communication link between the first security station and the at least second security station [0159].

As to claim 2, Monroe discloses that the providing the security data to the at least second security station comprises transmitting the security data over an electronic network (i.e. forwarding the security data) [0108].

As to claim 3, Monroe discloses using a controller operably connected to the first security station to direct the security data to the at least second security station (i.e. devices are connected via a network) [0156].

As to claims 4 and 34, Monroe discloses that the selecting the at least second security station is based on pre-defined criteria (i.e. In those regions where automatic timers on lighting generate motion events, coordination between the light controls and the surveillance system is managed to prevent false alarms. This is accomplished by having the alarm system control the lights and by using different criteria for event detection with the lights on versus lights off. Also, the alarm system can be configured to sense the signal controlling the lights to confirm that such a video change is authorized at that time. Cameras that have sufficient sensitivity and/or auxiliary illumination sources such as small bulbs or infrared illuminators can be used such that video surveillance may continue with normal lighting off.) [0166].

As to claim 5, Monroe discloses that the predefined criteria includes the availability of an operator at the at least second security station (i.e. Administrators and roaming guards or security personnel may be equipped with a PDA that is connected via wireless LAN with high data bandwidths and with no common carrier access charges when the PDA is within range of the access points providing connectivity between the PDA and the LAN hosting the system.) [0198].

As to claim 6, Monroe discloses that the predefined criteria comprises an expertise of an operator of the at least second security station [0198].

As to claim 7, Monroe discloses that providing the communication link between the at least first security station and the at least second security station comprises providing a graphical overlay on images in the collected security data (i.e. A graphic drawing tool to draw around areas on a scene that are to be considered or not considered for trigger events can generate a custom sector, or can select a set of predefined sectors that are used to create "the best" mask fitting the scenario. An example of excluding motion detection by masking is a window in an outside door that is desired to be masked such that it does not detect motion. An example of including motion detection by masking would be aiming a camera on paintings in a museum at an oblique angle, and setting masking such that any motion in the area of the painting would generate a motion trigger. The creation "zones" are monitored by combination of cameras and/or camera sectors. Zones can be activated or deactivated independently.) [0175].

As to claim 8, Monroe discloses that the opening the communication link between the first security station and the at least second security station comprises providing a bi-directional audio link between the first security station and the at least second security station [0198].

As to claim 9, Monroe discloses that the opening the communication link between the first security station and the at least second security station comprises providing a video link between the first security station and the at least second security station [0112].

As to claim 10, Monroe discloses controlling security data collection equipment from the at least second security station [0108].

As to claims 14 and 31, Monroe discloses that the collecting security data comprises collecting fire detection data from a sensor [0136].

As to claims 15 and 26, Monroe discloses that the opening a communication link includes opening a communication link over an electronic network [0109].

As to claims 16 and 27, Monroe discloses that providing the security data to the at least second security station, comprises providing the security data to the at least second security station over an electronic network using an internet protocol [0108].

As to claim 19, Monroe discloses that selecting at least a second security station, comprises selecting at least a second security station located remotely from the first security station [0108].

As to claim 20, Monroe discloses that collecting security data comprises collecting security data with equipment controlled from the first security station [0108].

As to claim 21, Monroe discloses that the opening a communication link between the first security station and the at least second security station, comprises opening a bi-directional data transfer link [0108].

As to claim 23, Monroe discloses a system comprising:

> a security data collection unit (i.e. forwarding the event to selected stations on a network. Basically, the location, type and priority of event are "tagged" at the point where a sensor picks up the event and event data is then forwarded only to selected stations on the network as required by a priority hierarchy. This permits a large amount of data to be collected at the site of a sensor while minimizing transmission of the data to an "as-needed" basis, reducing the overall bandwidth requirements of the system. As an example, while periodic data may be gathered at a sensor, only data indicating a change in condition will be transmitted to

various monitoring stations. In addition, monitoring stations are selected based on pre-established hierarchy, typically managed by a system server) [0108];

a first viewing unit to display the collected security data (i.e. The database holds a record of images, motion, triggers, alarms, and event processing actions that have been taken. As the database is searched and/or played back forward, reverse, fast or slow, all of the associated information such as images, motion levels, triggers, alarms, and event processing can be displayed in synchrony with each other. After the fact information can be added at specific time locations also, such as Word Files, Power Point Images, e-mails, and the like. These can then become part of the master database recording information about image events. In addition to collected data, created data may also be retrieve. For example, the histogram may be retrieved from the database, wherein the histogram shows the data in the same manner as it did when created. The playback can be in real time, faster, or slower than real time. Playback can also be forward or backward. This permits searching for "trigger" events in the database, then playing back in real time, faster, or slower than real time.) [0135];

a second viewing unit to display the collected security data concurrently with the display on the first viewing unit (i.e. When the user selects the EVENTS button, the system displays a box that allows the user to configure the various event notification functions. This control box is illustrated in FIG. 9. As shown, the alarm control Panel provides three selection tabs: Profiles, Alarms, and Alerts. In FIG. 9, the Profiles tab has been selected. The system displays the current

alarm profiles for which the system has been configured, and provides options for the user to Edit the existing profile, Remove it, or Add a new profile. Button 225 allows the user to arm or disarm the alarm functions of the system.) [0220]; and

a controller to selectively direct collected security data to the second viewing unit [0159].

As to claim 24, Monroe discloses that the controller selectively directs the collected security data to the second viewing unit upon a signal of a viewer of the first viewing unit [0108].

As to claim 25, Monroe discloses a communication link between a security station and at least one supervisor station [0198].

As to claim 30, Monroe discloses that the first viewing unit is located remotely from the second viewing unit [0198].

As to claim 33, Monroe discloses a security data collection unit controller operably connected to the second viewing unit (i.e. PDA's) [0109].

As to claim 35, Monroe discloses that the pre-defined criteria comprises an availability of an operator of the second viewing unit [0198].

As to claim 36, Monroe discloses that the pre-defined criteria comprises an expertise of an operator of the second viewing unit [0198].

As to claim 37, Monroe discloses a communication unit enabling an operator of the second viewing unit to communicate with a subject of the collected security data [0109].

As to claim 38, Monroe discloses that the collected security data includes data added by an operator of the first viewing unit [0175].

As to claim 39, Monroe discloses a first security data collection unit controller operably connected to the first viewing unit, and a second security data collection unit operably connected to the second viewing unit [0108].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 11, 13, 40 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe US 2003/0025599 A1 as applied to claim 1 above, and further in view of O'Hara US 2003/0058084 A1.

As to claims 11, 13, 40 and 41, Monroe discloses the at least second security station (i.e. closed circuit television systems and alarm systems) [0237].

Monroe does not teach that controlling security data collection equipment comprises controlling at least one biometric sensor from the at least one of the security stations.

O'Hara teaches a biometric characteristic airport security system 100. The system 100 is comprised of a check-in terminal 102 (also considered to be a ticketing terminal) and a gate terminal 104 that communicate with each other through a data network 106. The data network 106 to which the check-in terminal and the gate terminal 104 are coupled enables the ticketing terminal 102 and the gate terminal 104 to share data with each other as well as a server 108, which among other things functions as a repository of data collected and processed as described

hereinafter and which is embodied as one or more computers and associated storage devices, known to those of ordinary skill in the art [0016].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Monroe so that one of the security stations would have been a biometric sensor.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Monroe by the teaching of O'Hara because it allows for a record to be generated of a person that can now be compared against a database of terrorist/criminal/most wanted/etc. [0002].

9. Claims 12 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe US 2003/0025599 A1 as applied to claims 1 and 23 above, and further in view of Modica et al US 2003/0023592 A1 (hereinafter Modica).

As to claims 12 and 32, Monroe discloses the at least second security station (i.e. closed circuit television systems and alarm systems) [0237]

Monroe does not teach that the collecting security data comprises collecting security data from a baggage x-ray machine operated by an individual.

Modica teaches an x-ray screening system 102 containing a video monitor 104 that displays x-ray images of objects 108 to an operator 106. Certain elements in FIG. 2 are generally similar to elements in FIG. 1 but may be referenced by different numerals. Typically, objects 108 pass through system 102 on a conveyor 110. As discussed below, the current invention involves various databases for providing, storing and transmitting information. Existing types of databases

and means for providing communication between such databases may be used with the invention [0031].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Monroe so that one of the security stations would have been an x-ray machine that would have had means for providing, storing and transmitting information.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Monroe by the teaching of Modica because it provides a means to track the types of threats a system operator has seen and detected, as well as the difficulty of the threats the operator has seen [0016].

10. Claims 17, 18, 28 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe US 2003/0025599 A1 as applied to claims 1 and 23 above, and further in view of Sullivan U.S. Patent No. 7,015,945 B1.

As to claims 17, 18, 28 and 29, Monroe discloses opening a communication link between the first security station and the at least second security station (i.e. forwarding the event to selected stations on a network. Basically, the location, type and priority of event are "tagged" at the point where a sensor picks up the event and event data is then forwarded only to selected stations on the network as required by a priority hierarchy. This permits a large amount of data to be collected at the site of a sensor while minimizing transmission of the data to an "as-needed" basis, reducing the overall bandwidth requirements of the system. As an example, while periodic data may be gathered at a sensor, only data indicating a change in condition will be transmitted

to various monitoring stations. In addition, monitoring stations are selected based on pre-established hierarchy, typically managed by a system server) [0108].

Monroe does not teach opening a videoconference link between the first security station and the at least second security station.

Sullivan teaches that if controller 76 detects alarm condition 85 from alarm 83 at step 312, client 12 establishes communication with server 20 or optionally alarm monitoring station 28 at step 314. While client 12 maintains alarm condition 85, client 12 and server 20 or station 28 exchange data, video, and audio at step 316 to implement a one-way or two-way audio/video conferencing link for remote surveillance, management, or supervision. If alarm condition 85 persists at step 318, client 12 and server 20 or station 28 continue to exchange data 82, video 72, and audio 74 at step 316. If alarm condition 85 is over at step 318 and the operation of client 12 is not done at step 320, the method returns to process the next financial transaction at step 300 [column 8, lines 4-16]. Sullivan suggests that a videoconferencing link that is based on an ITU.F323 protocol. Sullivan suggests that the videoconference link is based on a ITU.H323 protocol.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Monroe so that the video surveillance would have included a one-way or two-way audio/video conferencing in the event an alarm condition is detected.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Monroe by the teaching of Sullivan because it provides

real-time or near real-time alerts in the case an alarm condition is generated [column 3, lines 41-51].

11. Claims 22 and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Monroe US 2003/0025599 A1 as applied to claims 1 and 23 above, and further in view of Korosec US 2003/0056113 A1.

As to claims 22 and 42, Monroe discloses collecting security data. Monroe discloses a sensor picks up the event and event data is then forwarded only to selected stations on the network as required by a priority hierarchy. This permits a large amount of data to be collected at the site of a sensor while minimizing transmission of the data to an "as-needed" basis, reducing the overall bandwidth requirements of the system. As an example, while periodic data may be gathered at a sensor, only data indicating a change in condition will be transmitted to various monitoring stations. In addition, monitoring stations are selected based on pre-established hierarchy, typically managed by a system server [0108].

Monroe does not teach that the collecting security data comprises calculating a height of a feature of a subject from an image of the subject

Korosec teaches measuring attributes such as DNA fingerprint and/or profile, ethnicity, citizenship, religious affiliation, political affiliation, biometric data, height, weight, health status (e.g., failure to have particular disease(s)), gender, registration status with Selective Service, history of conviction of felony and/or inclusion on list(s) of governmental agencies and/or private groups [0032].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Monroe so that biometric attributes would have been measure. Height of the individual would have been one of the attributes.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Monroe by the teaching of Korosec because it provides a device that facilitates identifying an individual to a regulated authorization system [0006].

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/
Examiner, Art Unit 2131

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131